

REMARKS/ARGUMENTS

Reconsideration and allowance of this application are respectfully requested.

Currently, claims 1, 4-26 and 29-31 are pending in this application.

Request for Return of Fully Initialed Form PTO-1449:

An Information Disclosure Statement (IDS) including a copy of the PCT International Search Report and a Form PTO-1449 was filed on September 14, 2000. The Form PTO-1449 was returned along with the Office Action. Two of the four documents cited in the Form PTO-1449 were initialed as being considered by the Examiner. The other two documents cited in the Form PTO-1449, however, were not initialed as being considered by the Examiner. Applicant has therefore attached hereto a copy of the partially initialed Form PTO-1449 which lists the uninitialed documents (WO 97/2661 and EP 0 528 730). While EP 0 528 730 is written in a non-English language, Applicant notes that U.S. Patent No. 5,301,233 is a corresponding publication (see, e.g., the patent family annex, Form PCT/ISA/210). Applicant respectfully requests that the Examiner fully initial and return the Form PTO-1449 as an indication that all of the cited documents have been considered.

Request to Confirm Receipt of Applicant's Priority Documents:

The present application is a national phase filing of international application no. PCT/GB98/03753 designating the US. The Notification of Acceptance of Application Under 35 U.S.C. §371 and 37 CFR 1.494 or 1.495 (Form PCT/DO/EO/903) mailed June 27, 2000 expressly acknowledges receipt of the priority documents. The Office Action acknowledges Applicant's claim for foreign priority under 35 U.S.C. §119. However, the

Office Action (Form PTOL-326) indicates that only “some” of the certified copies of the priority documents have been received. (See section 12 of Form PTOL-326). In light of the earlier acknowledgement by the USPTO that the priority documents have properly been received by the USPTO via WIPO and the PCT practice, the Examiner is respectfully requested to review the application and confirm that in fact all of Applicant’s priority documents have been properly received so as to perfect Applicant’s priority claim under 35 U.S.C. §119. At the very least, Applicant respectfully requests an indication of which certified copies of priority documents have allegedly not been received by the USPTO.

Rejection Under 35 U.S.C. §102:

Claims 1-28 were rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Ming et al (U.S. ‘815, hereinafter “Ming”). Applicant respectfully traverses this rejection with respect to still pending claims 1 and 4-26.

For a reference to anticipate a claim, each element must be found, either expressly or under principles of inherency, in the reference. Applicant submits that Ming fails to disclose each element of the claimed invention. For example, Ming fails to disclose “at the secure module of the or each selected user, in response to the said control message, controlling the availability of keys generated from the seed value, thereby controlling access by the users to the said data,” as required by independent claim 1 and its dependents. Similarly, Ming fails to disclose “in response to the said control message, controlling the availability of keys generated using the said seed value and thereby controlling access by the user of the customer terminal to data received at the customer

terminal,” as required by independent claim 11 and its dependents. Ming also fails to disclose “control means arranged to only release keys for decrypting those respective frames for which a control field is received, and being arranged to, in response to the said control messages in the control fields, control the availability to the users of keys generated from the seed value,” as required by independent claim 12 and its dependents.

As an example, claim 1 requires that a seed value for key generation is communicated to a secure module of a user. The secure module then generates keys from the seed value in response to control messages sent with data frames. The keys are used to decode the data frames. In such an arrangement, providing the secure module with the seed value has thus given it the ability to decode the received data frames. The control message which will determine whether or not the secure module performs decoding are sent (e.g., at a later time) with the data frames.

In contrast, Ming discloses a decoder in which the output to a video monitor is inhibited in response to control messages sent with the frames, but this is not achieved via a secure module which controls the availability of keys to control access to data as claimed. In Ming’s system, the video data frames are decoded, and the decoded data is subsequently withheld from output to the monitor (see, *e.g.*, col. 8, lines 56-57 and col. 10, lines 20-22). In particular, the Verification/Authorization unit 208 of Ming’s system governs whether the data will be displayed upon the video monitor (col. 24, lines 8-11), but this operates on the relevant video frames only after they have been decoded by the video-audio descrambler 207 (as indicated in the layout of Fig. 17).

The Office Action apparently alleges that col. 17, lines 35-46 discloses the above claimed features. (See page 3, lines 14-16 of the Office Action). Applicant respectfully disagrees. Col. 17, lines 35-46 states:

“As shown in FIG. 8, when the address field is equal to 4h-7h, the corresponding 32 bits of data field entries indicate which classes of users are authorized to receive the present programming. Up to 32 classes of users are supported, with each class corresponding to a bit position, b_0 - b_{31} . For each of the 32 bit positions within these four data bytes, a logical ‘1’ indicates that a corresponding class of subscribers is authorized to receive the present programming. Moreover, for each bit position, a logical ‘0’ indicates that a corresponding class of subscribers is not authorized to receive the present programming.”

Ming’s system is therefore much different from the arrangement required by the present invention, in which any decoding of data frames that a user is unauthorized to receive can be prevented using the control messages. The unavailability of the keys in the present application prevents the decoding of the affected frames. The prevention mechanism of the present invention can therefore be considered to operate at an earlier stage of the decoding process, and as a result can provide a more secure system. In the present invention, the item required to be secure is the key generation module, whereas in Ming, the entire video decoder must be secure to prevent the output from the descrambler from simply being re-routed to the monitor, thereby bypassing the authorization module. In addition, since only the key generation module is required to be secure (instead of the entire decoder), less processing power is required for the secure components to operate, thereby enabling their provision by low-processing components such as smart cards and the like. Ming also does not suggest any particular security problems with its

arrangement which might lead one of ordinary skill in the art to modify its system to arrive at the present invention.

The above cited portion of Ming discloses control messages which are integrated into an address field of the transmitted data to signify those users who are authorized to receive the present programming. While this portion of Ming states that some subscribers are not authorized to receive the present programming, it is silent as to how that prevention is achieved. In particular, what this portion of Ming fails to disclose is a secure module which controls (e.g., stops) the release of keys in response to the control messages, thereby controlling (e.g., preventing) decryption of data frames. In contrast, the only mechanism by which Ming prevents the subscriber from receiving the program is by preventing the already decoded data from being output to the monitor (col. 8, lines 56-57). While the final data output received by the monitor may be the same, the mechanism by which this is achieved is not the same.

Col. 10, lines 45-53 of Ming (specifically identified on page 4, lines 1-4 of the Office Action) also fails to disclose or suggest controlling the availability of keys in response to a control message to thereby control decryption of data frames. Col. 10, lines 45-53 states the following:

“For example, the data output to the keycard may include a key value. The remaining data output to the keycard will each be applied to a prestored permutation table. Each permuted value derived from the permutation table will be exclusive-ORed with the key value, from which a single bit for the keycard's output value is extracted. As a result, a particular result, or signature value is determined, which is a function of the particular sequence of values input from the decoder apparatus.”

The above portion of Ming describes a secure module (a keycard) which functions as a signature analyzer to confirm that a user is authorized to receive the programming. However, in the event that the user is not authorized, the device simply precludes the display of the video data as described in col. 10, lines 60-61. There is no teaching or suggestion of controlling the availability of keys in response to control messages required to decrypt data frames.

Accordingly, Applicant submits that claims 1 and 4-26 are not anticipated by Ming and therefore respectfully requests that the rejection of these claims under 35 U.S.C. §102 be withdrawn.

New Claims:

New claims 29-31 have been added to provide additional protection for the invention. Since new claims 29, 30 and 31 depend from independent claims 1, 11 and 12, respectively, these new claims are allowable for at least the reasons discussed above with respect to these independent claims.

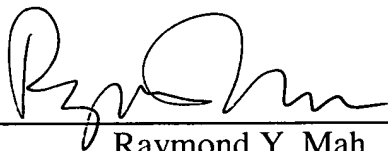
FAIRMAN et al.
Application No. 09/555,929
March 22, 2004

Conclusion:

Applicant believes that this entire application is in condition for allowance and respectfully requests a notice to this effect. If the Examiner has any questions or believes that an interview would further prosecution of this application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
Raymond Y. Mah
Reg. No. 41,426

RYM:sl
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4044
Facsimile: (703) 816-4100

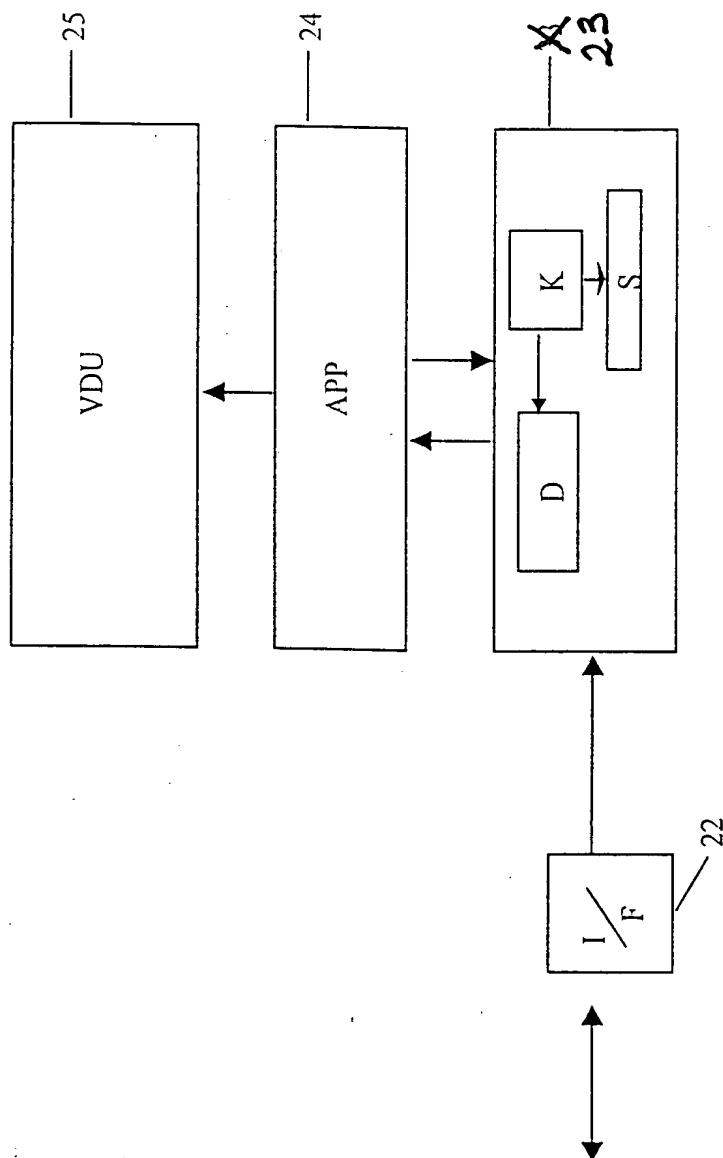


Figure 2

